CLAIMS

WHAT IS CLAIMED IS:

1. A method of booting a computer system, the method comprising:

establishing a secret between two or more devices; and

securing the secret in each of the two or more devices.

2. The method of claim 1, wherein establishing the secret between two or more devices comprises providing a first GUID from a first device to a master device; and

wherein securing the secret in each of the two or more devices comprises storing the first GUID in a GUID table in the master device, preventing access to the first GUID in the first device, and preventing access to the GUID table in the master device.

3. The method of claim 2, further comprising:

the first device setting an introduced bit in response to providing the first GUID from the first device to the master device.

4. The method of claim 2, wherein establishing the secret between two or more devices further comprises providing a system GUID from a master device to at least a first device; and wherein securing the secret in each of the two or more devices further comprises storing the system GUID in a storage location in at least the first device, preventing access to the system GUID in the storage location in at least the first device, and preventing access to the system GUID in the master device.

5. The method of claim 1, wherein establishing the secret between two or more devices comprises providing a system GUID from a master device to at least a first device; and

wherein securing the secret in each of the two or more devices comprises storing the system GUID in a storage location in at least the first device, preventing access to the system GUID in the storage location in at least the first device, and preventing access to the system GUID in the master device.

6. The method of claim 5, further comprising:

the first device setting an introduced bit in response to providing the system GUID from the master device to at least the first device.

7. The method of claim 1, wherein establishing the secret between two or more devices comprises a master device providing a value to a first device as a first GUID; and wherein securing the secret in each of the two or more devices comprises the first device storing the first GUID in a storage location, the master device storing the first GUID in a GUID table, preventing access to the first GUID in the first device, and preventing access to the GUID table in the master device.

8. The method of claim 7, wherein establishing the secret between two or more devices further comprises the master device obtaining a random number and the master device providing the random number to the first device as the first GUID.

9. A method for booting a computer system, the method comprising:

step for establishing a secret between two or more devices; and

step for securing the secret in each of the two or more devices.

10. The method of claim 9, wherein the step for establishing the secret between two or more devices comprises step for providing a first GUID from a first device to a master device; and

wherein the step for securing the secret in each of the two or more devices comprises step for storing the first GUID in a GUID table in the master device, step for preventing access to the first GUID in the first device, and step for preventing access to the GUID table in the master device.

11. The method of claim 10, further comprising:

step for the first device setting an introduced bit in response to the step for providing the first GUID from the first device to the master device.

12. The method of claim 10, wherein the step for establishing the secret between two or more devices further comprises step for providing a system GUID from a master device to at least a first device; and wherein the step for securing the secret in each of the two or more devices further comprises step for storing the system GUID in a storage location in at least the first device, step for preventing access to the system GUID in the storage location in at least the first device, and step for preventing access to the system GUID in the master device.

13. The method of claim 9, wherein the step for establishing the secret between two or more devices comprises step for providing a system GUID from a master device to at least a first device; and wherein the step for securing the secret in each of the two or more devices comprises step for storing the system GUID in a storage location in at least the first device, step for preventing access to the system GUID in the storage location in at least the first device, and step for preventing access to the system GUID in the master device.

14. The method of claim 13, further comprising:

step for the first device setting an introduced bit in response to providing the system GUID from the master device to at least the first device.

15. The method of claim 9, wherein the step for establishing the secret between two or more devices comprises step for a master device providing a value to a first device as a first GUID; and wherein the step for securing the secret in each of the two or more devices comprises step for the first device storing the first GUID in a storage location, step for the master device storing the first GUID in a GUID table, step for preventing access to the first GUID in the first device, and step for preventing access to the GUID table in the master device.

16. The method of claim 15, wherein the step for establishing the secret between two or more devices further comprises step for the master device obtaining a random number and step for the master device providing the random number to the first device as the first GUID.

17. A computer readable program storage device encoded with instructions that, when executed by a computer system, performs a method of booting the computer system, the method comprising:

establishing a secret between two or more devices; and

securing the secret in each of the two or more devices.

18. The computer readable program storage device of claim 17, wherein establishing the secret between two or more devices comprises providing a first GUID from a first device to a master device; and

wherein securing the secret in each of the two or more devices comprises storing the first GUID in a GUID table in the master device, preventing access to the first GUID in the first device, and preventing access to the GUID table in the master device.

19. The computer readable program storage device of claim 18, the method further comprising:

the first device setting an introduced bit in response to providing the first GUID from the first device to the master device.

20. The computer readable program storage device of claim 18, wherein establishing the secret between two or more devices further comprises providing a system GUID from a master device to at least a first device; and wherein securing the secret in each of the two or more devices further comprises storing the system GUID in a storage location in at least the first device, preventing access to the system GUID in the storage location in at least the first device, and preventing access to the system GUID in the master device.

21. The computer readable program storage device of claim 17, wherein establishing the secret between two or more devices comprises providing a system GUID from a master device to at least a first device; and wherein securing the secret in each of the two or more devices comprises storing the system GUID in a storage location in at least the first device, preventing access to the system GUID in the storage location in at least the first device, and preventing access to the system GUID in the master device.

22. The computer readable program storage device of claim 21, the method further comprising:

the first device setting an introduced bit in response to providing the system GUID from the master device to at least the first device.

23. The computer readable program storage device of claim 17, wherein establishing the secret between two or more devices comprises a master device providing a value to a first device as a first GUID; and wherein securing the secret in each of the two or more devices comprises the first device storing the first GUID in a storage location, the master device storing the first GUID in a GUID table, preventing access to the first GUID in the first device, and preventing access to the GUID table in the master device.

24. The computer readable program storage device of claim 23, wherein establishing the secret between two or more devices further comprises the master device obtaining a random number and the master device providing the random number to the first device as the first GUID.

25. A method of booting a computer system, the computer system including a processor coupled to a memory, to security hardware, and to a first device, the method comprising:

processing BIOS code instructions;

accessing security hardware;

accessing a first device;

locking the security hardware; and

calling boot code.

26. The method of claim 25, wherein accessing security hardware includes the BIOS code instructions accessing the security hardware.

27. The method of claim 25, wherein accessing security hardware includes the first device accessing the security hardware.

28. The method of claim 25, wherein locking the security hardware includes locking the security hardware to prevent access to the first device.

29. The method of claim 28, wherein locking the security hardware to prevent access to the first device includes setting one or more lock bits to prevent access to the first device.

30. The method of claim 25, further comprising:
unlocking the security hardware.

31 The method of claim 30, wherein unlocking the security hardware includes unlocking the security hardware in response to accessing the first device.

32. The method of claim 25, further comprising:
checking a lock status of the security hardware.

33. The method of claim 32, wherein checking the lock status of the security hardware comprises reading one or more entries in a storage location configured to store one or more lock bits.

34. A method for booting a computer system, the computer system including a processor coupled to a memory, to security hardware, and to a first device, the method comprising:

step for processing BIOS code instructions;

step for accessing security hardware;

step for accessing a first device;

step for locking the security hardware; and

step for calling boot code.

35. The method of claim 34, wherein the step for accessing the security hardware includes step for the BIOS code instructions accessing the security hardware.

36. The method of claim 34, wherein the step for accessing the security hardware includes step for the first device accessing the security hardware.

37. The method of claim 34, wherein the step for locking the security hardware includes step for locking the security hardware to prevent access to the first device.

38. The method of claim 37, wherein the step for locking the security hardware to prevent access to the first device includes step for setting one or more lock bits to prevent access to the first device.

39. The method of claim 34, further comprising:

step for unlocking the security hardware.

40 The method of claim 39, wherein the step for unlocking the security hardware includes step for unlocking the security hardware in response to the step for accessing the first device.

41. The method of claim 34, further comprising:

step for checking a lock status of the security hardware.

42. The method of claim 41, wherein the step of checking the lock status of the security hardware comprises step for reading one or more entries in a storage location configured to store one or more lock bits.

43. A computer readable program storage device encoded with instructions that, when executed by a computer system including a processor coupled to a memory, to security hardware, and to a first device, performs a method of booting the computer system, the method comprising:

processing BIOS code instructions;

accessing security hardware;

accessing a first device;

locking the security hardware; and

calling boot code.

44. The computer readable program storage device of claim 43, wherein accessing the security hardware includes the BIOS code instructions accessing the security hardware.

45. The computer readable program storage device of claim 43, wherein said accessing security hardware includes the first device accessing the security hardware.

46. The computer readable program storage device of claim 43, wherein said locking the security hardware includes locking the security hardware to prevent access to the first device.

47. The computer readable program storage device of claim 46, wherein locking the security hardware to prevent access to the first device includes setting one or more lock bits to prevent access to the first device.

48. The computer readable program storage device of claim 43, the method further comprising:

unlocking the security hardware.

49 The computer readable program storage device of claim 48, wherein unlocking the security hardware includes unlocking the security hardware in response to accessing the first device.

50. The computer readable program storage device of claim 43, the method further comprising:

checking a lock status of the security hardware.

51. The computer readable program storage device of claim 50, wherein checking the lock status of the security hardware comprises reading one or more entries in a storage location configured to store one or more lock bits.

52. A method of booting a personal computer system, the method comprising:

reading a secret from a first location;

storing the secret in a secure location different from the first location; and

locking the first location.

53. The method of claim 52, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from a memory;

wherein storing the secret in a secure location different from the first location comprises storing the secret in a secure location different from the memory; and

wherein locking the first location comprises locking the memory

54. The method of claim 53, wherein the memory is a read-only memory (ROM);

wherein reading a secret from a memory comprises reading the secret from the ROM; and

wherein securing the secret in a secure location different from the memory comprises securing the secret in the secure location different from the ROM.

55. The method of claim 54, wherein the data comprises basic input-output system (BIOS) data and the ROM is a BIOS ROM configured to store the BIOS data;

wherein reading the secret from the ROM comprises reading the secret from the BIOS ROM; and

wherein securing the secret in the secure location different from the ROM comprises securing the secret in the secure location different from the BIOS ROM.

56. The method of claim 55, wherein securing the secret in the secure location different from the memory comprises storing the secret in SMM memory space.

57. The method of claim 52, further comprising:

reading code from the first location, wherein the code is different from the secret and different from the data stored in the first location.

58. The method of claim 57, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from a memory;

wherein storing the secret in a secure location different from the first location comprises storing the secret in a secure location different from the memory;

wherein locking the first location comprises locking the memory; and

wherein reading the code from the first location, wherein the code is different from the secret and different from the data stored in the first location comprises reading the code from the memory, wherein the code is different from the secret and different from the data stored in the memory.

59. The method of claim 58, wherein securing the secret in a secure location different from the memory comprises storing the secret in SMM memory space.

60. A method for booting a personal computer system, the method comprising:

step for reading a secret from a first location;

step for storing the secret in a secure location different from the first location; and

step for locking the first location.

61. The method of claim 60, wherein the first location comprises a memory;

wherein the step for reading the secret from the first location comprises step for reading the secret from a memory;

wherein the step for storing the secret in the secure location different from the first location comprises step for storing the secret in a secure location different from the memory; and

wherein the step for locking the first location comprises step for locking the memory.

62. The method of claim 61, wherein the memory is a read-only memory (ROM);

wherein the step for reading the secret from the memory comprises reading the secret from the ROM; and

wherein the step for securing the secret in the secure location different from the memory comprises securing the secret in the secure location different from the ROM.

63. The method of claim 62, wherein the data comprises basic input-output system (BIOS) data and the ROM is a BIOS ROM configured to store the BIOS data;

wherein the step for reading the secret from the ROM comprises step for reading the secret from the BIOS ROM; and

wherein the step for securing the secret in the secure location different from the ROM comprises step for securing the secret in the secure location different from the BIOS ROM.

64. The method of claim 63, wherein the step for securing the secret in the secure location different from the memory comprises step for storing the secret in SMM memory space.

65. The method of claim 60, further comprising:

step for reading code from the first location, wherein the code is different from the secret and different from the data stored in the first location.

66. The method of claim 65, wherein the first location comprises a memory;

wherein the step for reading the secret from the first location comprises step for reading the secret from the memory;

wherein the step for storing the secret in the secure location different from the first location comprises step for storing the secret in the secure location different from the memory;

wherein the step for locking the first location comprises step for locking the memory; and

wherein the step for reading the code from the first location, wherein the code is different from the secret and different from the data stored in the first location comprises step for reading the code from the memory, wherein the code is different from the secret and different from the data stored in the memory.

67. The method of claim 66, wherein the step for securing the secret in the secure location different from the memory comprises step for storing the secret in SMM memory space.

68. A computer readable program storage device encoded with instructions that, when executed by a personal computer system, performs a method of booting the personal computer system, the method comprising:

reading a secret from a first location;

storing the secret in a secure location different from the first location; and

locking the first location.

69. The computer readable program storage device of claim 68, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from a memory;

wherein storing the secret in a secure location different from the first location comprises storing the secret in a secure location different from the memory; and

wherein locking the first location comprises locking the memory

70. The computer readable program storage device of claim 69, wherein the memory is a read-only memory (ROM);

wherein reading a secret from a memory comprises reading the secret from the ROM; and

wherein securing the secret in a secure location different from the memory comprises securing the secret in the secure location different from the ROM.

71. The computer readable program storage device of claim 70, wherein the data comprises basic input-output system (BIOS) data and the ROM is a BIOS ROM configured to store the BIOS data;

wherein reading the secret from the ROM comprises reading the secret from the BIOS ROM; and

wherein securing the secret in the secure location different from the ROM comprises securing the secret in the secure location different from the BIOS ROM.

72. The computer readable program storage device of claim 71, wherein securing the secret in the secure location different from the memory comprises storing the secret in SMM memory space.

73. The computer readable program storage device of claim 68, the method further comprising:

reading code from the first location, wherein the code is different from the secret and different from the data stored in the first location.

74. The computer readable program storage device of claim 73, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from a memory;

wherein storing the secret in a secure location different from the first location comprises storing the secret in a secure location different from the memory;

wherein locking the first location comprises locking the memory; and

wherein reading the code from the first location, wherein the code is different from the secret and different from the data stored in the first location comprises reading the code from the memory, wherein the code is different from the secret and different from the data stored in the memory.

75. The computer readable program storage device of claim 74, wherein securing the secret in a secure location different from the memory comprises storing the secret in SMM memory space.

76. A method of booting a computer system, the method comprising:

requesting authentication for a device;

receiving authentication for the device; and

setting a timer associated with the device.

77. The method of claim 76, wherein requesting authentication for the device comprises requesting authentication for the device from a subsystem; and wherein receiving authentication for the device comprises receiving authentication for the device from the subsystem.

78. The method of claim 76, further comprising:

requesting authentication for a subsystem;

receiving authentication for the subsystem; and

setting a timer associated with the subsystem.

79. The method of claim 78, wherein requesting authentication for the subsystem comprises requesting authentication for the subsystem from the computer system; and wherein receiving authentication for the subsystem comprises receiving authentication for the subsystem from the computer system.

80. The method of claim 76, further comprising:

requesting authentication for the computer system;

receiving authentication for the computer system; and

setting a timer associated with the computer system.

81. The method of claim 80, wherein requesting authentication for the computer system comprises requesting authentication for the computer system from a network security authenticator; and wherein receiving authentication for the computer system comprises receiving authentication for the computer system from the network security authenticator.

82. The method of claim 76, wherein the device comprises the computer system, wherein requesting authentication for the device comprises requesting authentication for the computer system from a network security authenticator; and wherein receiving authentication for the computer system comprises receiving authentication for the device from the network security authenticator.

83. A method for booting a computer system, the method comprising:

step for requesting authentication for a device;

step for receiving authentication for the device; and

step for setting a timer associated with the device.

84. The method of claim 83, wherein the step for requesting authentication for the device comprises step for requesting authentication for the device from a subsystem; and wherein the step for receiving authentication for the device comprises step for receiving authentication for the device from the subsystem.

85. The method of claim 83, further comprising:

step for requesting authentication for a subsystem;

step for receiving authentication for the subsystem; and

step for setting a timer associated with the subsystem.

86. The method of claim 85, wherein the step for requesting authentication for the subsystem comprises step for requesting authentication for the subsystem from the computer system; and wherein the step for receiving authentication for the subsystem comprises step for receiving authentication for the subsystem from the computer system.

87. The method of claim 83, further comprising:

step for requesting authentication for the computer system;

step for receiving authentication for the computer system; and

step for setting a timer associated with the computer system.

88. The method of claim 87, wherein the step for requesting authentication for the computer system comprises step for requesting authentication for the computer system from a network security authenticator; and wherein the step for receiving authentication for the computer system comprises step for receiving authentication for the computer system from the network security authenticator.

89. The method of claim 83, wherein the device comprises the computer system, wherein the step for requesting authentication for the device comprises step for requesting authentication for the computer system from a network security authenticator; and wherein

the step for receiving authentication for the computer system comprises step for receiving authentication for the device from the network security authenticator.

90. A computer readable program storage device encoded with instructions that, when executed by a computer system, performs a method of booting the computer system, the method comprising:

requesting authentication for a device;

receiving authentication for the device; and

setting a timer associated with the device.

91. The computer readable program storage device of claim 90, wherein requesting authentication for the device comprises requesting authentication for the device from a subsystem; and wherein receiving authentication for the device comprises receiving authentication for the device from the subsystem.

92. The computer readable program storage device of claim 90, the method further comprising:

requesting authentication for a subsystem;

receiving authentication for the subsystem; and

setting a timer associated with the subsystem.

93. The computer readable program storage device of claim 92, wherein requesting authentication for the subsystem comprises requesting authentication for the subsystem from the computer system; and wherein receiving authentication for the subsystem comprises receiving authentication for the subsystem from the computer system.

94. The computer readable program storage device of claim 90, the method further comprising:

requesting authentication for the computer system;

receiving authentication for the computer system; and

setting a timer associated with the computer system.

95. The computer readable program storage device of claim 94, wherein requesting authentication for the computer system comprises requesting authentication for the computer system from a network security authenticator; and wherein receiving authentication for the computer system comprises receiving authentication for the computer system from the network security authenticator.

96. The computer readable program storage device of claim 90, wherein the device comprises the computer system, wherein requesting authentication for the device comprises requesting authentication for the computer system from a network security authenticator; and wherein receiving authentication for the computer system comprises receiving authentication for the device from the network security authenticator.

97. A method of booting a computer system, the method comprising:

requesting authentication for a device;

failing authentication for the device; and

preventing access to the device upon failing authentication for the device.

98. The method of claim 97, wherein the device is the computer system; wherein requesting authentication for the device comprises requesting authentication for the computer system; wherein failing authentication for the device comprises failing authentication for the computer system; and wherein preventing access to the device upon failing authentication for the device comprises preventing access to the computer system upon failing authentication for the computer system.

99. The method of claim 98, wherein requesting authentication for the computer system comprises requesting authentication for the computer system over a network from a network authentication device.

100. A method for booting a computer system, the method comprising:

step for requesting authentication for a device;

step for failing authentication for the device; and

step for preventing access to the device upon failing authentication for the device.

101. The method of claim 100, wherein the device is the computer system; wherein the step for requesting authentication for the device comprises step for requesting authentication for the computer system; wherein the step for failing authentication for the device comprises step for failing authentication for the computer system; and wherein the step for preventing access to the device upon failing authentication for the device comprises step for preventing access to the computer system upon failing authentication for the computer system.

102. The method of claim 101, wherein the step for requesting authentication for the computer system comprises step for requesting authentication for the computer system over a network from a network authentication device.

103. A computer readable program storage device encoded with instructions that, when executed by a computer system, performs a method of booting the computer system, the method comprising:

requesting authentication for a device;

failing authentication for the device; and

preventing access to the device upon failing authentication for the device.

104. The computer readable program storage device of claim 103, wherein the device is the computer system; wherein requesting authentication for the device comprises requesting authentication for the computer system; wherein failing authentication for the device comprises failing authentication for the computer system; and wherein preventing access to the device upon failing authentication for the device comprises preventing access to the computer system upon failing authentication for the computer system.

105. The computer readable program storage device of claim 104, wherein requesting authentication for the computer system comprises requesting authentication for the computer system over a network from a network authentication device.

106. A method of booting a computer system, the method comprising:

requesting authentication through security hardware using master mode;

placing one or more bus interface logics in master mode by setting master mode bits therein;

receiving authentication data through the one or more bus interface logics in master mode; and

verifying the authentication data.

107. The method of claim 106, further comprising:

exiting master mode and flushing buffers in the one or more bus interface logics.

108. The method of claim 106, further comprising:

ending booting the computer system if the authentication data is not verified.

109. The method of claim 106, further comprising:

continuing booting the computer system after the authentication data is verified.

110. A method for booting a computer system, the method comprising:

step for requesting authentication through security hardware using master mode;

step for placing one or more bus interface logics in master mode by setting master mode bits therein;

step for receiving authentication data through the one or more bus interface logics in master mode; and

step for verifying the authentication data.

111. The method of claim 110, further comprising:

step for exiting master mode and flushing buffers in the one or more bus interface logics.

112. The method of claim 110, further comprising:

step for ending booting the computer system if the authentication data is not verified.

113. The method of claim 110, further comprising:

step for continuing booting the computer system after the authentication data is verified.

114. A computer readable program storage device encoded with instructions that, when executed by a computer system, performs a method of booting the computer system, the method comprising:

requesting authentication through security hardware using master mode;

placing one or more bus interface logics in master mode by setting master mode bits therein;

receiving authentication data through the one or more bus interface logics in master mode; and

verifying the authentication data.

115. The computer readable program storage device of claim 114, further comprising:

exiting master mode and flushing buffers in the one or more bus interface logics.

116. The computer readable program storage device of claim 114, further comprising:

ending booting the computer system if the authentication data is not verified.

117. The computer readable program storage device of claim 114, further comprising:

continuing booting the computer system after the authentication data is verified.